UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/473,522	12/28/1999	KENNETH A. PARULSKI	78744PRC	1080

1333	7590	05/31/2006

PATENT LEGAL STAFF
EASTMAN KODAK COMPANY
343 STATE STREET
ROCHESTER, NY 14650-2201

EXAMINER
GYORFI, THOMAS A

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 05/31/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>*17 May 2006*</u>.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-25* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-25* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
    Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

1.   Claims 1-25 remain for examination. The correspondence filed 4/7/06 amended
claims 1, 6-10, and 22.

2.   Any statements of Official Notice made by Examiner in the previous Office Action
that were not challenged by Applicant are now taken as admissions of prior art, as per
MPEP 2144.03(c).

Continued Examination Under 37 CFR 1.114

3.   A request for continued examination under 37 CFR 1.114, including the fee set
forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this
application is eligible for continued examination under 37 CFR 1.114, and the fee set
forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action
has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 4/7/06
has been entered.

Response to Arguments

4.   Applicant's arguments with respect to claims 1-25 have been considered but are
moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

5.   The text of those sections of Title 35, U.S. Code not included in this action can
be found in a prior Office action.

6.   For purposes of the obviousness rejections herein, it is noted that the Noll patent

is fully incorporated by reference into the Silverbrook disclosure as a component of the

latter invention (Silverbrook, col. 204, lines 10-20).

7.   Claims 1-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Safai et al (U.S. Patent 6,167,469), Silverbrook et al (U.S. Patent 6,788,336), Noll et al.

(U.S. Patent 5,732,138), and Eastlake et al. (RFC1750: "Randomness

Recommendations for Security"; hereinafter, "Eastlake").

Referring to Claim 1:

     Safai discloses a digital camera of the type employing a private key to encrypt a

hash of a digital image captured by the digital camera to produce an image

authentication signature, the improvement comprising: (a) a processor located within

the digital camera for generating private key and a public key (col. 4, lines 1-15; col. 7,

lines 30-40; Claim 29); and (b) means for storing the private key in a memory in the

digital camera for subsequent use in encryption of the hash of the digital image to

produce the image authentication signature (col. 16, lines 1-10, 20-35).

     Safai does not explicitly teach "generating a random seed and for using the

random seed to generate a private key and a public key."

     Silverbrook discloses a processor located within a digital camera that generates

a random seed (col. 189, lines 45-55; col. 173, line 35 – col. 175, line 2) and teaches

using a random seed to generate keys (col. 151, lines 12-13; col. 193, line 25 – col.

195, line 25).

It would have been obvious to one of ordinary skill in the art at the time the
invention was made to incorporate the teachings of Silverbrook regarding a digital
camera generating a random seed and using the random seed to generate keys into the
digital camera disclosed by Safai in order to allow it to create the required public and
private keys. The motivation for doing so would be to potentially increase the security of
the camera by generating keys that cannot be easily compromised by guessing (col.
153, lines 15-20).

Although the preferred embodiment of the Lavarand process as employed by
Silverbrook uses an image of lava lamps captured by an image sensor of a digital
camera as a chaotic source of randomness, Noll teaches that alternate embodiments
are permitted (Noll, col. 4, lines 43-45). A number of alternate sources of chaotic
randomness similar to the claimed subject matter are suggested, including both random
noise from an electronic component and using an image sensor of a camera to digitize
images of various random [natural] phenomena (Ibid, and also col. 1, line 55 – col. 2,
line 5). Nevertheless, Eastlake teaches that even prior to the existence of the Noll
method, it was well known to digitize the noise from an image sensor of a camera for
use as a chaotic source of randomness specifically for the purpose of generating
cryptographic keys (Eastlake, Abstract and page 13, section 5.3.1, 1st paragraph). It
would have been obvious to one of ordinary skill in the art at the time the invention was
made to use the noise generated entirely by the image sensor of a digital camera such
as those of Silverbrook and Safai as the chaotic source of randomness for the camera's
Lavarand component. The motivation for doing so is threefold: [1] secure cryptographic

keys are more likely to be generated through the use of true randomness rather than

pseudo-randomness (Eastlake, Abstract; and page 10, "5. Hardware for Randomness",

1st paragraph); [2] any source of randomness can be improved by the Noll method for

the purpose of cryptographic key generation, in the event that the chaotic source does

not always return truly random results (Noll, col. 2, lines 20-25 and col. 3, lines 5-25);

and [3] it would obviate the need for a user of a camera employing Silverbrook's

disclosed technology to carry additional cumbersome hardware to avail oneself of the

novel features of that invention, instead relying solely on an internal component already

known to be present (Silverbrook, col. 1, lines 49-51).

Referring to Claims 6 and 22:

Safai discloses a method of producing an image authentication signature in a

digital camera employing a private key to encrypt a hash of an image captured by the

digital camera, the improvement comprising the steps of:

(a) generating a private key in the digital camera (col. 4, lines 1-15; col. 7, lines

30-40; Claim 29); and

(b) storing the private key in a memory in the digital camera for subsequent

encryption of the hash of the digital image (col. 16, lines 1-10, 20-35).

Safai does not explicitly teach "generating a random seed from a physically

random process in the digital camera and using the random seed to generate a private

key and a public key."

Silverbrook discloses generating a random seed (col. 189, lines 45-55; col. 173,

line 35 – col. 175, line 2) using a physically random process (col. 204, lines 10-20) and

using a random seed to generate keys (col. 151, lines 12-13; col. 193, line 25 – col.

195, line 25).

It would have been obvious to one of ordinary skill in the art at the time the

invention was made to incorporate the teachings of Silverbrook regarding a digital

camera generating a random seed and using the random seed to generate keys into the

digital camera disclosed by Safai in order to allow it to create the required private key.

The motivation for doing so would be to potentially increase the security of the camera

by generating keys that cannot be easily compromised by guessing (col. 153, 15-20).

Although the preferred embodiment of the Lavarand process as employed by

Silverbrook uses an image of lava lamps captured by an image sensor of a digital

camera as a chaotic source of randomness, Noll teaches that alternate embodiments

are permitted (Noll, col. 4, lines 43-45). A number of alternate sources of chaotic

randomness similar to the claimed subject matter are suggested, including both random

noise from an electronic component and using an image sensor of a camera to digitize

images of various random [natural] phenomena (Ibid, and also col. 1, line 55 – col. 2,

line 5). Nevertheless, Eastlake teaches that even prior to the existence of the Noll

method, it was well known to digitize the noise from an image sensor of a camera for

use as a chaotic source of randomness specifically for the purpose of generating

cryptographic keys (Eastlake, Abstract and page 13, section 5.3.1, 1st paragraph). It

would have been obvious to one of ordinary skill in the art at the time the invention was

made to use the noise generated entirely by the image sensor of a digital camera such

as those of Silverbrook and Safai as the chaotic source of randomness for the camera's

Lavarand component. The motivation for doing so is threefold: [1] secure cryptographic

keys are more likely to be generated through the use of true randomness rather than

pseudo-randomness (Eastlake, Abstract; and page 10, "5. Hardware for Randomness",

1st paragraph); [2] any source of randomness can be improved by the Noll method for

the purpose of cryptographic key generation, in the event that the chaotic source does

not always return truly random results (Noll, col. 2, lines 20-25 and col. 3, lines 5-25);

and [3] it would obviate the need for a user of a camera employing Silverbrook's

disclosed technology to carry additional cumbersome hardware to avail oneself of the

novel features of that invention, instead relying solely on an internal component already

known to be present (Silverbrook, col. 1, lines 49-51).

Referring to Claim 7:

Safai discloses a method of authenticating an image captured by a digital

camera, comprising the steps of:

(a) generating a private key and a public key in the digital camera (col. 4, lines 1-

15; col. 7, lines 30-40; Claim 29);

(b) storing the private key in a memory in the digital camera (col. 16, lines 1-10,

20-35);

(c) communicating the public key to a user (col. 4, lines 5-15);

(d) capturing a digital image (col. 5, lines 35-45; col. 15, lines 60-65);

(e) hashing the captured digital image in the digital camera to produce an image hash (col. 16, lines 1-10);

(f) encrypting the image hash in the digital camera with the private key to produce a digital signature (col. 16, lines 20-35); and

(g) authenticating the digital image by hashing the image outside of the digital camera, decrypting the digital signature using the public key to produce a decrypted signature, and comparing the decrypted signature with the image hash produced outside of the digital camera (col. 16, lines 10-20).

Safai does not explicitly teach "generating a random seed in the digital camera and using the random seed to generate a private key and a public key."

Silverbrook discloses generating a random seed (col. 189, lines 45-55; col. 173, line 35 – col. 175, line 2) and using a random seed to generate keys (col. 151, lines 12-13, col. 193, line 25 – col. 195, line 25).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teachings of Silverbrook regarding a digital camera generating a random seed and using the random seed to generate keys into the digital camera disclosed by Safai in order to allow it to create the required public key and private key. The motivation for doing so would be to potentially increase the security of the camera by generating keys that cannot be easily compromised by guessing (col. 153, lines 15-20).

Although the preferred embodiment of the Lavarand process as employed by Silverbrook uses an image of lava lamps captured by an image sensor of a digital

camera as a chaotic source of randomness, Noll teaches that alternate embodiments are permitted (Noll, col. 4, lines 43-45). A number of alternate sources of chaotic randomness similar to the claimed subject matter are suggested, including both random noise from an electronic component and using an image sensor of a camera to digitize images of various random [natural] phenomena (Ibid, and also col. 1, line 55 – col. 2, line 5). Nevertheless, Eastlake teaches that even prior to the existence of the Noll method, it was well known to digitize the noise from an image sensor of a camera for use as a chaotic source of randomness specifically for the purpose of generating cryptographic keys (Eastlake, Abstract and page 13, section 5.3.1, 1st paragraph). It would have been obvious to one of ordinary skill in the art at the time the invention was made to use the noise generated entirely by the image sensor of a digital camera such as those of Silverbrook and Safai as the chaotic source of randomness for the camera's Lavarand component. The motivation for doing so is threefold: [1] secure cryptographic keys are more likely to be generated through the use of true randomness rather than pseudo-randomness (Eastlake, Abstract; and page 10, "5. Hardware for Randomness", 1st paragraph); [2] any source of randomness can be improved by the Noll method for the purpose of cryptographic key generation, in the event that the chaotic source does not always return truly random results (Noll, col. 2, lines 20-25 and col. 3, lines 5-25); and [3] it would obviate the need for a user of a camera employing Silverbrook's disclosed technology to carry additional cumbersome hardware to avail oneself of the novel features of that invention, instead relying solely on an internal component already known to be present (Silverbrook, col. 1, lines 49-51).

Referring to Claim 8:

Safai discloses a method of manufacturing a digital camera capable of producing a digital signature useful for image authentication, comprising the steps of:

(a) manufacturing a digital camera with an internal processor for generating a public key and private key, storing the private key in a memory in the digital camera and communicating the public key to a camera operator (col. 16, lines 20-40);

(b) sending the digital camera to an authentication service (col. 15, lines 15-25);

(c) activating the digital camera at the authentication service to produce the public key and private key, and registering the public key at the authentication service (col. 15, lines 15-25; col. 16, lines 20-40); and

(d) sending the digital camera to a user (e.g. col. 1, lines 37-47).

Safai does not explicitly teach "generating a random seed in the digital camera and using the random seed to generate a private key and a public key."

Silverbrook discloses generating a random seed (col. 189, lines 45-55; col. 173, line 35 – col. 175, line 2) and using a random seed to generate keys (col. 151, lines 12-13; col. 193, line 25 – col. 195, line 25).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teachings of Silverbrook regarding a digital camera generating a random seed and using the random seed to generate keys into the digital camera disclosed by Safai in order to allow it to create the required private key. The motivation for doing so would be to potentially increase the security of the camera by generating keys that cannot be easily compromised by guessing (col. 153, 15-20).

Although the preferred embodiment of the Lavarand process as employed by

Silverbrook uses an image of lava lamps captured by an image sensor of a digital

camera as a chaotic source of randomness, Noll teaches that alternate embodiments

are permitted (Noll, col. 4, lines 43-45). A number of alternate sources of chaotic

randomness similar to the claimed subject matter are suggested, including both random

noise from an electronic component and using an image sensor of a camera to digitize

images of various random [natural] phenomena (Ibid, and also col. 1, line 55 – col. 2,

line 5). Nevertheless, Eastlake teaches that even prior to the existence of the Noll

method, it was well known to digitize the noise from an image sensor of a camera for

use as a chaotic source of randomness specifically for the purpose of generating

cryptographic keys (Eastlake, Abstract and page 13, section 5.3.1, 1st paragraph). It

would have been obvious to one of ordinary skill in the art at the time the invention was

made to use the noise generated entirely by the image sensor of a digital camera such

as those of Silverbrook and Safai as the chaotic source of randomness for the camera's

Lavarand component. The motivation for doing so is threefold: [1] secure cryptographic

keys are more likely to be generated through the use of true randomness rather than

pseudo-randomness (Eastlake, Abstract; and page 10, "5. Hardware for Randomness",

1st paragraph); [2] any source of randomness can be improved by the Noll method for

the purpose of cryptographic key generation, in the event that the chaotic source does

not always return truly random results (Noll, col. 2, lines 20-25 and col. 3, lines 5-25);

and [3] it would obviate the need for a user of a camera employing Silverbrook's

disclosed technology to carry additional cumbersome hardware to avail oneself of the

novel features of that invention, instead relying solely on an internal component already

known to be present (Silverbrook, col. 1, lines 49-51).

Referring to Claim 9:

Safai discloses a digital camera of the type employing a private key to encrypt a

hash of a digital image captured by the digital camera to produce an image

authentication signature and a metadata signature corresponding to one or more

metadata values, the improvement comprising:

(a) a processor located within the digital camera for generating a public key and

a private key (col. 4, lines 1-15; col. 7, lines 30-40; Claim 29); and

(b) means for storing the private key in a memory in the digital camera for

subsequent use in encryption of the hash of the digital image to produce the image

authentication signature and the metadata signature (col. 16, lines 1-10, 20-35).

Safai does not explicitly teach "generating a random seed in the digital camera

and using the random seed to generate a private key and a public key."

Silverbrook discloses generating a random seed (col. 189, lines 45-55; col. 173,

line 35 – col. 175, line 2) and using a random seed to generate keys (col. 151, lines 12-

13; col. 193, line 25 – col. 195, line 25).

It would have been obvious to one of ordinary skill in the art at the time the

invention was made to incorporate the teachings of Silverbrook regarding a digital

camera generating a random seed and using the random seed to generate keys into the

digital camera disclosed by Safai in order to allow it to create the required private key.

The motivation for doing so would be to potentially increase the security of the camera

by generating keys that cannot be easily compromised by guessing (col. 153, 15-20).

Although the preferred embodiment of the Lavarand process as employed by

Silverbrook uses an image of lava lamps captured by an image sensor of a digital

camera as a chaotic source of randomness, Noll teaches that alternate embodiments

are permitted (Noll, col. 4, lines 43-45). A number of alternate sources of chaotic

randomness similar to the claimed subject matter are suggested, including both random

noise from an electronic component and using an image sensor of a camera to digitize

images of various random [natural] phenomena (Ibid, and also col. 1, line 55 – col. 2,

line 5). Nevertheless, Eastlake teaches that even prior to the existence of the Noll

method, it was well known to digitize the noise from an image sensor of a camera for

use as a chaotic source of randomness specifically for the purpose of generating

cryptographic keys (Eastlake, Abstract and page 13, section 5.3.1, 1st paragraph). It

would have been obvious to one of ordinary skill in the art at the time the invention was

made to use the noise generated entirely by the image sensor of a digital camera such

as those of Silverbrook and Safai as the chaotic source of randomness for the camera's

Lavarand component. The motivation for doing so is threefold: [1] secure cryptographic

keys are more likely to be generated through the use of true randomness rather than

pseudo-randomness (Eastlake, Abstract; and page 10, "5. Hardware for Randomness",

1st paragraph); [2] any source of randomness can be improved by the Noll method for

the purpose of cryptographic key generation, in the event that the chaotic source does

not always return truly random results (Noll, col. 2, lines 20-25 and col. 3, lines 5-25);

and [3] it would obviate the need for a user of a camera employing Silverbrook's

disclosed technology to carry additional cumbersome hardware to avail oneself of the

novel features of that invention, instead relying solely on an internal component already

known to be present (Silverbrook, col. 1, lines 49-51).

Referring to Claim 10:

Safai discloses a method of producing an image authentication signature in a

digital camera, comprising the steps of:

(a) capturing a digital image (col. 15, lines 60-65);

(b) compressing the captured digital image (col. 14, lines 15-25);

(c) generating, a public key and private key in the digital camera (col. 4, lines 1-

15; col. 7, lines 30-40; Claim 29);

(d) storing the private key in a memory in the digital camera (col. 16, lines 1-10,

20-35);

(e) providing one or more metadata values (col. 16, lines 1-15);

(f) hashing the compressed captured digital image and at least one of the

metadata values to produce an image hash (col. 16, lines 1-10); and

(g) encrypting the image hash to produce the image authentication signature (col.

16, lines 20-30).

Safai does not explicitly teach "generating a random seed in the digital camera

and using the random seed to generate a private key and a public key."

Silverbrook discloses generating a random seed (col. 189, lines 45-55; col. 173, line 35 – col. 175, line 2) and using a random seed to generate keys (col. 151, lines 12-13; col. 193, line 25 – col. 195, line 25).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teachings of Silverbrook regarding a digital camera generating a random seed and using the random seed to generate keys into the digital camera disclosed by Safai in order to allow it to create the required private key. The motivation for doing so would be to increase the security of the camera by generating keys that cannot be easily compromised by guessing (col. 153, lines 15-20).

Although the preferred embodiment of the Lavarand process as employed by Silverbrook uses an image of lava lamps captured by an image sensor of a digital camera as a chaotic source of randomness, Noll teaches that alternate embodiments are permitted (Noll, col. 4, lines 43-45). A number of alternate sources of chaotic randomness similar to the claimed subject matter are suggested, including both random noise from an electronic component and using an image sensor of a camera to digitize images of various random [natural] phenomena (Ibid, and also col. 1, line 55 – col. 2, line 5). Nevertheless, Eastlake teaches that even prior to the existence of the Noll method, it was well known to digitize the noise from an image sensor of a camera for use as a chaotic source of randomness specifically for the purpose of generating cryptographic keys (Eastlake, Abstract and page 13, section 5.3.1, 1st paragraph). It would have been obvious to one of ordinary skill in the art at the time the invention was made to use the noise generated entirely by the image sensor of a digital camera such

as those of Silverbrook and Safai as the chaotic source of randomness for the camera's

Lavarand component. The motivation for doing so is threefold: [1] secure cryptographic

keys are more likely to be generated through the use of true randomness rather than

pseudo-randomness (Eastlake, Abstract; and page 10, "5. Hardware for Randomness",

1st paragraph); [2] any source of randomness can be improved by the Noll method for

the purpose of cryptographic key generation, in the event that the chaotic source does

not always return truly random results (Noll, col. 2, lines 20-25 and col. 3, lines 5-25);

and [3] it would obviate the need for a user of a camera employing Silverbrook's

disclosed technology to carry additional cumbersome hardware to avail oneself of the

novel features of that invention, instead relying solely on an internal component already

known to be present (Silverbrook, col. 1, lines 49-51).

Referring to Claim 2:

Safai, Silverbrook, Noll, and Eastlake disclose all the limitations of claim 1 above.

Silverbrook further discloses an image sensor for capturing images (element 2 of Figure

2) and wherein the processor includes means for producing a random seed for the

private key by processing an image captured from the image sensor so that the random

noise level in the captured image is used in producing the random seed (col. 173, line

35 – col. 175, line 2; col. 193, line 25 – col. 195, line 25; col. 204, lines 10-20).

Referring to Claims 3 and 25:

Safai, Silverbrook, Noll, and Eastlake disclose the limitations of claims 2 and 22

above. Safai further discloses

(i) a variable gain amplifier coupled to the image sensor (col. 5, lines 45-60);

(ii) an analog-to-digital converter coupled to the variable gain amplifier and the

processor for producing digital signals corresponding to the captured images (col. 5,

lines 50-60); and

(iii) the processor causing the variable gain amplifier to be in a high gain

condition when the initial test image is captured (col. 5, lines 55-60).

Referring to Claim 4:

Safai, Silverbrook, Noll, and Eastlake disclose the limitations of claim 1 above.

Silverbrook further discloses wherein the processor includes one or more algorithms for

producing a random seed, wherein the random seed is used to produce a random

number k, and for using the random number k to create the image authentication

signature by hashing the raw image data prior to image processing (col. 173, line 35 –

col. 175, line 2; col. 193, line 25 – col. 195, line 25; col. 204, lines 10-20).

Referring to Claim 5:

Safai, Silverbrook, Noll, and Eastlake disclose the limitations of claim 4 above.

Safai further discloses the processor includes an image processing algorithm which

uses JPEG compression (col. 14, lines 15-25).

Referring to Claim 11:

Safai, Silverbrook, Noll, and Eastlake disclose the limitations of Claim 10 above. Safai further discloses storing in an image file in the digital camera, the image authentication signature, the compressed digital image data, and the one or more metadata values (col. 12, lines 1-15; col. 14, lines 10-25; col. 16, lines 1-10).

Referring to Claim 12:

Safai, Silverbrook, Noll, and Eastlake disclose the limitations of Claim 10 above. Safai further discloses the encrypting step includes encrypting the image hash with a private key produced in the digital camera to produce the image authentication signature (col. 16, lines 1-40).

Referring to Claim 13:

Safai, Silverbrook, Noll, and Eastlake disclose the limitations of Claim 10 above. Safai further discloses wherein the encrypting step includes encrypting the image hash with the private key to produce the image authentication signature (col. 16, lines 25-40); and further including the step of authenticating the captured digital image by hashing the compressed digital image outside of the digital camera, decrypting the image authentication signature using the public key to produce a decrypted signature, and comparing the decrypted signature with the image hash produced outside of the digital camera (col. 16, lines 10-25).

Referring to Claim 14:

Safai, Silverbrook, Noll, and Eastlake disclose the limitations of Claim 1 above.

Safai further hashing the uncompressed captured digital image to produce a random

number k (col. 16, lines 1-10); and wherein the encrypting step includes using the

random number k to produce the image authentication signature (col. 16, lines 20-35).

Referring to Claim 15:

Safai, Silverbrook, Noll, and Eastlake disclose the limitations of Claim 1 above.

Safai further discloses the encrypting step further produces a metadata signature

corresponding to one or more metadata values (col. 16, lines 1-10; col. 12, lines 50-60).

Regarding claims 16-21:

Safai, Silverbrook, Noll, and Eastlake disclose the limitations of Claims 1 and 6-

10 above. Safai also discloses firmware memory, wherein the private key is produced

using an algorithm stored in the firmware memory (col. 7, lines 50-55).

Neither Safai nor Silverbrook explicitly disclose "wherein the algorithm is deleted

from the firmware memory after the private key is generated." However, Silverbrook

teaches that an attacker could gain control of the program [algorithm] used to generate

a random seed and use it to reverse engineer a private key, while not being authorized

to do so (col. 155, line 55-60). This suggests that it would be desirable to delete the

algorithm used to generate a private key after the unique private key for a digital camera

has been generated. Furthermore, Silverbrook also teaches that another method of

defeating the protection afforded by the authentication chip is to reverse engineer the

chip so as to determine the inner workings of the algorithms contained therein (col. 156,

lines 55-60). In addition, as noted previously by Applicant, Silverbrook discloses that

the keys should only be produced at the place of manufacture, implying that the

consumers/end-users has no valid reason to possess any means to create or alter keys

themselves (e.g. col. 200, lines 30-45). All of these facts suggest that it would have

been obvious to one of ordinary skill in the art at the time the invention was made to

modify the combination of Safai and Silverbrook [and Noll and Eastlake] to delete the

algorithm from the firmware memory after the private key is generated, in order to

prevent it from falling into the wrong hands.

Regarding claim 23:

Safai, Silverbrook, Noll, and Eastlake disclose all the limitations of claim 22

above. Silverbrook further discloses including an image sensor for capturing images,

and wherein the physically random process is dependent upon a random seed

produced from a random noise level in a captured image (col. 204, lines 10-20).

Regarding claim 24:

Safai, Silverbrook, Noll, and Eastlake disclose all the limitations of claim 23

above. It is now taken as Applicant admitted prior art that the random images taken by

the image sensor in the Silverbrook disclosure would necessarily contain random dark

fields [relative to other portions of the image that are lighter in color], and that this data

would necessarily be incorporated into the random number generated by the disclosed

process (see the Office action of 7/12/05, page 5). Alternatively, Eastlake discloses this

limitation (page 14, section 5.3.1, 1st paragraph).

Conclusion

8.   The prior art made of record and not relied upon is considered pertinent to

applicant's disclosure: the web page "Landon Curt Noll's Bookmarks" cites Eastlake as

relevant to the Noll invention, further supporting a motivation to combine teachings.

9.   Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Tom Gyorfi whose telephone number is (571) 272-3849.

The examiner can normally be reached on 8:30am - 5:00pm Monday - Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the

organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free).

TAG
5/17/06
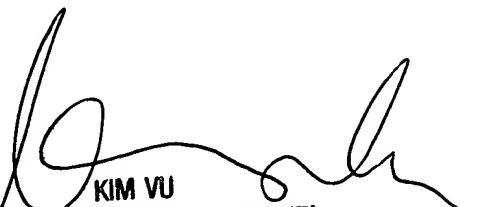
KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100